



OFFICE OF THE STAFF JUDGE ADVOCATE

Legal Issues and Information Operations

Tom King AFSC-JA

(520) 533-3197

DSN: 821-3197

Kingto@hqasc.army.mil



OVERVIEW

- **Constitutional Basis**
- **Statutory Framework**
- **Limits On Network Monitoring Activity**



BACKGROUND FOR LEGAL ISSUES

- **U.S. Constitution**
 - **4th amendment (protection from unreasonable search and seizure)**
 - **1st amendment (free speech issues)**
- **Variety of Legal Issues; Generally Untested in the Courts - No clear boundaries**



KEY STATUTES

- **Electronic Communications Privacy Act (Public Law 99-508) (1986)**
- **Foreign Intelligence Surveillance Act (Public Law 95-511) (1978)**
- **Computer Fraud and Abuse Act (Public Law 98-473) (1986)**



OFFICE OF THE STAFF JUDGE ADVOCATE

Electronic Communications Privacy Act

18 USC 2510-2521 and 2701

- **The Wiretap (Title III) Statute**
- **Prohibits Unauthorized Interception, Use, or Disclosure of Wire, Oral or Electronic Communications**
- **Limited Exceptions are Found in the Statute**
- **Stored Communications protected**



ECPA EXCEPTIONS

- **Service Provider [18 USC 2511(2)(a)(I)&(H)(ii)]
-To Protect Service or Rights & Property**
- **One Party Consent [18 USC 2511(2)(c)]**
- **Business Extension [18 USC 2510(5)(a)(1)]**
- **Pursuant to Legal Process (Warrant)**



OFFICE OF THE STAFF JUDGE ADVOCATE

ECPA EXCEPTIONS CONTINUED

- **COMSEC activities conducted in accordance with Attorney General Approved Procedures**



OFFICE OF THE STAFF JUDGE ADVOCATE

SERVICE PROVIDER EXCEPTION

- **Make sure your system is working and secure (like the telephone company)**
- **. . . May intercept, use or disclose communications while engaged in any activity which is necessarily incident to the rendition of the service or the protection of the rights or property of the service provider**
- **Army Guidance on these limits found in AR 380-19, Appendix G**



CONSENT TO MONTOR

- **May Be Express or Implied, But Implied is Weaker**
- **Look at ALL the Circumstances**
O'Connor v. Ortega 480 US 709 (1987)
- **O'Conner also established the right to privacy in the government work place.**



OFFICE OF THE STAFF JUDGE ADVOCATE

CONSENT

EXPRESS OR IMPLIED

Express Consent

- **Explicit Verbal or Written Permission**
- **Signed User Agreements**
- **Consent form**

Implied Consent

- **Warning Banners**
- **Policy Letters**
- **Orientation Briefings**
- **Notices in Bulletins or Newspapers**



OFFICE OF THE STAFF JUDGE ADVOCATE

DISCLOSING INTERCEPTED COMMUNICATIONS

- **Limited Disclosure Under ECPA**
 - **Other Service Providers and Employees**
 - **Parties**
 - **Pursuant to Authority of Statute, Court Order or Foreign Intelligence Surveillance Act**
 - **To Law Enforcement If Information Appears to Pertain To Commission of Crime and Was Inadvertently Obtained**



OFFICE OF THE STAFF JUDGE ADVOCATE

COMPUTER FRAUD AND ABUSE ACT

- **18 USC 1030**
- **The “Hacker Statute”**
- **Other Traditional Criminal Statutes Also Address Computer crimes**



COMPUTER CRIMES

- **Knowingly Access a Computer Without Authorization or Exceed Authorized Access**
- **Intentionally Cause Damage or Recklessly Disregard Risk of Such Damage**
- **Fraudulent Transfer of Passwords**
- **Sliding Scale of Punishment**
- **Exception for Law Enforcement or Intelligence Agency**



OFFICE OF THE STAFF JUDGE ADVOCATE

Foreign Intelligence Surveillance Act

- **Allows Electronic Surveillance to Gather Foreign Intelligence**
- **Foreign Power or Agent of Such Power**
- **FISA Court Must Approve**
- **FBI and NSA are Key Players**
- **Prohibitions Against Conducting Electronic Surveillance of U.S. Citizens Unless Exceptions Apply**



OFFICE OF THE STAFF JUDGE ADVOCATE

CYBERSPACE RULES OF THE ROAD

- **Strict compliance with Law & Regulation**
- **Clearly Identify the Purpose of Monitoring**
- **Following correct procedure is always the safest approach**
- **Get permission of System Owner in Writing**
- **Use Procedures and Software that will give you a good audit trail**
- **Know when to call in Law Enforcement and Counter Intelligence**



REGULATIONS

1. AR 380-19 -

- **Appendix G sets guidelines and limits for System and Network Administrators**

2. AR 380-53 -

- **Who can conduct “Information Systems Security Monitoring” - ACERT and RCERT types**



OFFICE OF THE STAFF JUDGE ADVOCATE

•The System Administrator is not authorized to view, modify, delete or copy data files which are stored on the Automated Information System which are not part of the System Administrator's operation of the system except when:

- 1. Authorized by the user or file owner.**
- 2. Performing system backup and disaster recovery responsibilities.**
- 3. Performing anti-virus functions and procedures.**
- 4. Performing actions which are necessary to ensure the continued operation and system integrity of the AIS.**
- 5. Performing Actions as part of a properly authorized investigation.**



WHY WORRY?

- **Subject to Civil and Criminal Suit if You Exceed your Authority**
- **Under ECPA YOU can be sued by Party to the communication or someone Against whom the interception was directed**
- **BUT: The US Attorney (prosecutor) is guided by DOJ, which supports ECPA Exceptions we use**